Cybersecurity Incident Report

# Section 1 – Identify the Attack

Upon reviewing the network traffic, the web server experienced a large volume of TCP SYN requests originating from an unfamiliar IP address. These requests did not proceed to complete the TCP handshake, leaving the server waiting for acknowledgments that never arrived.  
  
This pattern is characteristic of a SYN flood attack, a type of Denial-of-Service (DoS) attack. The objective of such an attack is to deplete the server’s available resources and prevent legitimate users from accessing services.

# Section 2 – Explain the Impact

Under normal conditions, establishing a TCP connection requires a three-way handshake consisting of:  
1. The client sends a SYN request to the server.  
2. The server replies with a SYN-ACK packet.  
3. The client completes the process by sending an ACK.  
  
In a SYN flood attack, the attacker sends a large number of SYN requests without responding with ACKs. As a result, the server allocates resources for incomplete sessions, eventually exhausting its capacity to accept new connections.  
  
Logs confirm an excessive number of SYN packets from a single IP, with no completion of the handshake. This caused the website to become inaccessible to employees and customers.

# Conclusion and Recommendations

The web server was targeted by a SYN flood attack, leading to denial of service for legitimate users. Immediate actions taken include taking the server offline and blocking the attacker's IP address. However, since IP spoofing can bypass such blocks, further recommendations include:  
- Implementing SYN cookies to validate connection attempts  
- Setting connection limits per IP  
- Deploying a firewall or intrusion prevention system (IPS) with rate-limiting features  
- Monitoring network traffic for anomalies to identify and respond to threats quickly.